इंटरनेट मानक

Disclosure to Promote the Right To Information

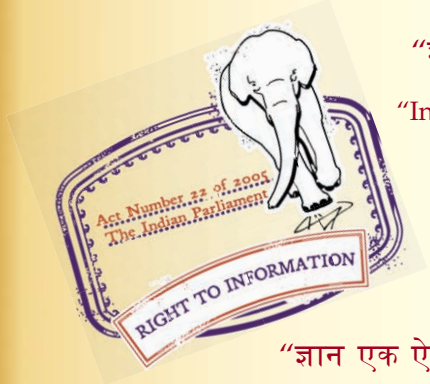
Whereas the Parliament of India has set out to provide a practical regime of right to information for citizens to secure access to information under the control of public authorities, in order to promote transparency and accountability in the working of every public authority, and whereas the attached publication of the Bureau of Indian Standards is of particular interest to the public, particularly disadvantaged communities and those engaged in the pursuit of education and knowledge, the attached public safety standard is made available to promote the timely dissemination of this information in an accurate manner to the public.

"जानने का अधिकार, जीने का अधिकार"
Mazdoor Kisan Shakti Sangathan
"The Right to Information, The Right to Live"

"पुराने को छोड नये के तरफ"
Jawaharlal Nehru
"Step Out From the Old to the New"

IS 15399 (2003): Hardware for Computers in the Safety System of Nuclear and Radiation Facilities [LITD 8: Electronic Measuring Instruments, Systems and Accessories]

"ज्ञान से एक नये भारत का निर्माण"
Satyanarayan Gangaram Pitroda
"Invent a New India Using Knowledge"



"ज्ञान एक ऐसा खजाना है जो कभी चुराया नहीं जा सकता है"
Bhartṛhari—Nītiśatakam
"Knowledge is such a treasure which cannot be stolen"

BLANK PAGE

PROTECTED BY COPYRIGHT

भारतीय मानक

नाभिकीय एवं विकिरण संयंत्रों की सुरक्षा प्रणाली में प्रयुक्त कंप्यूटरों के लिए हार्डवेयर

Indian Standard

HARDWARE FOR COMPUTERS IN THE SAFETY SYSTEM OF NUCLEAR AND RADIATION FACILITIES

ICS 27.120.20

© BIS 2003

BUREAU OF INDIAN STANDARDS
MANAK BHAVAN, 9 BAHADUR SHAH ZAFAR MARG
NEW DELHI 110002

October 2003

Price Group 7

FOREWORD

This Indian Standard was adopted by the Bureau of Indian Standards, after the draft finalized by the Nuclear Instrumentation Sectional Committee had been approved by the Electronics and Telecommunication Division Council.

Computer systems are extensively used for on line monitoring of the reactor core against blockage of coolant flow, on line power regulation, fuel handling operation, supervision of process parameters against safety thresholds, event sequence analysis, measurement of radiation level, etc. This standard gives the principles for the utilization of digital systems hardware for systems important to safety. This includes multiprocessor distributed systems and large-scale central processor systems constructed from off-the-shelf items or from newly developed hardware.

It lays down requirements specific to the hardware of digital systems. For specific requirements for computer software and common areas of hardware and software, IS 15398 : 2003 'Software for computers in the safety systems of nuclear and radiation facilities' is applicable.

For modules used in the design of a specific safety system application, relevant and auditable operating experience from nuclear or other applications as described in combination with quality assurance programmes of high reliability may be an acceptable method of qualification.

This standard may also be useful as a guide for other computer systems requiring real time applications.

This standard is based on IEC 987 (1989) 'Programmed digital computers important to safety for nuclear power stations' issued by the International Electrotechnical Commission.

The composition of the Committee responsible for formulation of this standard is given in Annex E.

Indian Standard

HARDWARE FOR COMPUTERS IN THE SAFETY SYSTEM OF NUCLEAR AND RADIATION FACILITIES

1 SCOPE

1.1 This standard is applicable to computer systems hardware for systems important to safety used in nuclear facilities. It is, therefore, applicable to safety systems and in general to safety-related systems.

1.2 The requirements specified are applicable but not restricted to the following items of such systems, down to the component level:

a) External power supplies to the computer system;

b) Internal architecture;

c) Input/Output equipment and interfaces;

d) Data transmission means;

e) Storage devices; and

f) Test devices to prove continued correct operation as far as any failure of these devices leads to failure of the computer system.

2 REFERENCES

The standards given in Annex A are necessary adjuncts to this standard.

3 TERMS AND DEFINITIONS

3.0 For the purpose of this standard, the following definitions shall apply:

3.1 Availability — The ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided.

3.2 Computer — A programmable functional unit that consists of one or more associated processing units and peripheral equipment, that is controlled by internally stored programmes and that can perform substantial computation, including numerous arithmetic operations or logic operations, without human intervention during a run.

3.3 Computer System — A system consisting of one or more computers (comprising hardware as well as software) collectively forming a functional unit of an instrumentation and control system.

3.4 Component

a) *Hardware* — Items from which the system is assembled (for example, integrated circuits, resistors, capacitors, wires, connectors, transistors, switches, etc.)

b) *Software* — A basic part of a programme.

3.5 Design — The theoretical work which leads towards a system requirements specification.

3.6 Development — The experimental test demonstration work which is intended to prove the success of any parts of the design whose performance cannot be ensured by theoretical work alone.

3.7 Diversity — The existence of different means of performing a required function (for example, other physical principles, other ways of solving the same task).

3.8 Guaranteed Power Supply — A power supply for the computer system which is designed to be able to provide satisfactory electrical supplies normally, during loss of electrical generator on the station, and during loss of connection of the station to the electrical distribution network or grid which it serves.

3.9 Integration Tests — Tests performed during the hardware/software integration process prior to computer system validation to verify compatibility of the software and the computer system hardware.

3.10 Maintainability — The probability that a given active maintenance action to an item under given conditions of use can be carried out within a stated time interval when the maintenance is performed under stated conditions and using stated procedures and resources.

3.11 Maintenance — The combination of all technical and administrative actions, including supervision actions, intended to retain an item in, or restore it to, a state in which it can perform a required function.

3.12 Module — Any assembly of interconnected components which constitutes an identifiable device, instrument or piece of equipment. A module can be removed as a unit and replaced with a spare. It has definable performance characteristics which permit it to be tested as a unit. A module could be a card, a draw out circuit breaker or any other sub-assembly of a larger device, provided it meets the requirements of this definition.

3.13 Qualified Life — The period of time for which satisfactory performance can be verified for a specified set of operating conditions.

3.14 Redundancy — The provision of alternative (identical or diverse) elements so that any one can

perform the required function regardless of the state of operation or failure of any other.

3.15 Reliability — The probability that a failure which causes deviation from the required output by more than specified tolerances, in a specific environment, does not occur during a specified exposure period.

3.16 Single Failure — A random failure, which results in the loss of capability of a component to perform its intended safety function. Consequential failures resulting from a single random occurrence are considered to be part of the single failure.

3.16.1 *Single Failure Criterion* — A criterion applied to a system such that it is capable of performing its safety task in the presence of any single failure.

3.17 Software — Programmes, procedures, rules and any associated documentation pertaining to the operation of a computer system.

3.18 Sub-system — A division of a system that in itself has the characteristics of a system.

3.19 System — A set of interconnected elements constituted to achieve a given objective by performing a specified function.

3.20 Validation — The test and evaluation of the integrated computer system (hardware and software) to ensure compliance with the functional, performance and interface requirements.

3.21 Verification — The process of determining whether or not the product of each phase of the digital computer system development process fulfills all the requirements imposed by the previous phase.

3.22 Application Programme— A computer programme that performs a task related to the process being controlled rather than the functioning of the computer itself.

3.23 Code Compaction — The purposeful reduction in memory size required for a computer programme by the elimination of redundant or extraneous instructions.

3.24 Computer Programme— A set of ordered instructions and data that specify operations in a form suitable for execution by a digital computer.

3.25 Data — A representation of facts, concepts or instructions in a formalized manner suitable for communication, interpretation or processing by a computer.

3.26 Defence in Depth — Provision of multiple levels of protection for ensuring safety of workers, the public or the environment.

3.27 Fault Tolerance — The built-in capability of a system to provide continued correct execution in the presence of a limited number of hardware or software faults.

3.28 Graceful Degradation — Stepwise reduction of system functions in response to detected failures while essential functions are maintained.

3.29 Initialize — To set counters, switches, addresses, or contents of storage devices to zero or other starting values at the beginning of, or at prescribed points in the operation of a computer programme.

3.30 Procedure — A portion of a computer programme which is named and which performs a specific task.

3.31 Software — Programmes, procedures, rules and any associated documentation pertaining to the operation of a computer system.

3.32 Software Life Cycle — The period of time that starts when a software product is conceived and ends when the product is no longer available for use. The software life cycle typically includes a requirements phase, design phase, implementation phase, test phase, installation and check-out phase, operation and maintenance phase.

3.33 Software Modification — Changes of already agreed documents leading to a change to the executable code or its data.

3.34 Software Modularity — The software attribute that provides a structure of highly independent computer programme units that are discrete and identifiable with respect to translating, testing and combining with other units.

4 PROJECT STRUCTURE

4.1 General

4.1.1 Any project will normally be divided up into a number of phases. Each phase is to some extent self-contained but will depend on other phases and will, in its turn, be depended on by others. These phases are informally recognizable by the specific activities pertinent to them. For applications important to safety, these phases shall be formalized and none of the identified phases shall be omitted. Some hardware and software phases may be performed simultaneously. Formalized procedures shall be defined to regulate the feedback between phases.

4.1.2 Project management documentation shall be provided to define the project sub-division so that the project can be run in a controlled manner with evolutions recorded and monitored. A quality assurance plan shall be applied.

4.2 Project Sub-division

The following general factors determine the activities in implementing a project:

a) The whole system life cycle (*see* Annex B) shall be considered.

b) Each phase of the system life cycle shall be divided into elementary tasks with a well defined activity for each of them.

c) Hardware products to be introduced into a phase shall be checked, verified and tested as appropriate before incorporation.

d) Adequate means (spare parts, devices for test or maintenance) and accommodation (laboratories, workshops, space, etc) shall be provided to carry out the tasks of each phase.

e) Each phase shall include generation of the appropriate documents.

f) Each phase shall be terminated by verification (*see* 7).

g) Every verification step shall result in a report on the analysis performed, the conclusions reached and any necessary changes decided. This report shall be included in the documentation.

h) The time schedule of the project shall be laid down with regard to:

1) facilitating feedback between hardware and software phases;

2) providing sufficient time for documentation, testing, verification, maintenance and quality assurance; and

3) giving a means for the recognition of difficulties which arise unexpectedly.

4.3 Quality Assurance

4.3.1 A hardware quality assurance plan shall exist as a part of the quality assurance plan for the computer system. It should include requirements for hardware which already has undergone a quality assurance procedure as well as for new hardware. The hardware quality assurance plan is closely connected to the licensing procedures. All activities during the computer lifetime executed by the plant operator, owner, contractors and sub-contractors shall be included.

This includes the following phases:

a) Design and development,

b) Procurement,

c) Manufacturing,

d) Construction and commissioning, and

e) Operation and maintenance.

4.3.2 The quality assurance plan shall describe the organization, management and execution of quality assurance orientated activities including:

a) Specifications control;

b) Design and design changes control;

c) Procurement control;

d) Control of instructions, procedures, drawings;

e) Document control;

f) Control of purchase material and services;

g) Identification and control of material;

h) Inspection;

j) Control of test equipment;

k) Control of handling/storage/shipping;

m) Inspection and testing status;

n) Monitoring of non-conformance and corrective actions;

p) Production of quality assurance records;

q) Audits; and

r) Environmental qualification conformance.

5 HARDWARE REQUIREMENTS

5.1 General

5.1.1 The hardware requirements shall be derived from the requirements of the systems important to safety and form part of the computer system specification. The computer system specification is a description of the combined hardware/software system and states the objectives and functions assigned to the computer system.

5.1.2 The hardware requirements shall be described in the hardware requirements specification.

5.1.3 The hardware requirements specification is part of the hardware documentation (*see* **14.2**).

5.1.4 Hardware requirements shall be presented according to a standard whose formality shall not preclude readability.

5.1.5 The requirements shall be unambiguous, testable, verifiable and achievable.

5.1.6 The hardware requirements specification shall be structured to give as an introduction, an overview of hardware requirements with a list of reference documents and the edition to be used and to identify the hardware functions important to safety.

5.1.7 The hardware functional and performance requirements, the reliability, the environmental and documentation requirements form the hardware requirements.

5.1.8 The hardware facilities for programme and data loading and checking as well as verification during start up and normal operation do not form an intrinsic part of the computer system required for continuous operation. The reliability requirements of **5.2** for these facilities may be different from those of the computer system.

5.1.9 The hardware requirements for computer systems include requirements which are applicable to hardware in general and requirements which are applicable to computer system hardware only.

5.1.10 The hardware requirements describe the product, not the project. The hardware requirements shall describe what has to be done and not how it has to be done. That is, the functions to be performed are described, rather than the means of implementation.

5.2 Functional and Performance Requirements

5.2.1 The hardware functional and performance requirements are derived from the functional and performance requirements of the systems important to safety. They shall be the result of a first design phase at system level allowing:

a) Definition of the overall architecture of the computer system and its division into sub-systems which fulfil the necessary functions;

b) Definition of the structural distribution of the sub-systems; and

c) Assignment of hardware performance requirements to these sub-systems.

5.2.2 The hardware functional and performance requirements, combined with the software requirements, shall be checked for compliance with the requirements for the systems important to safety.

5.2.3 All parts of the system, down to the component level, which contain built-in programmes shall be identified and the functions and programmes of those parts shall be appropriately specified in accordance with 7 of IS 15398.

5.2.4 The hardware functional requirements shall include, but are not restricted to, the definition of:

a) Purpose of the computer system hardware and each sub-system;

b) Structure of the computer system hardware;

c) Number and type of sensors and actuators to be connected to the computer system;

d) Characteristics of signals, such as, range, type, details needed for conversion from electrical range to physical range; and

e) Number and type of devices for the man/machine interface, such as, displays, printers and keyboards.

5.2.5 The hardware functional requirements shall clearly define the level at which a sub-system is to be integrated into the system. This definition shall identify for the sub-system, the relevant cabinet, frame, printed circuit board and integrated circuits. The design requirements will be selected on the basis of these levels (*see* **6**).

Each component or sub-system delivered by a supplier and which is to be integrated into the system shall be accompanied by a complete specification.

5.2.6 The hardware performance requirements shall include but are not restricted to the definition of:

a) Data acquisition rate;

b) Data handling capability;

c) Computation and data transmission speed;

d) Computation and conversion accuracy;

e) Noise rejection;

f) Response time; and

g) Irrationality check for input signal.

The performance requirements for the design of sub-systems shall be selected on the basis of the levels mentioned in **5.2.5**.

5.2.7 The hardware functional and performance requirements and mutual constraints between hardware and software shall be checked for feasibility and for the allowance of installed spare capacity, at an early phase of the project, to avoid the need for later changes.

5.3 Reliability Requirements

5.3.1 The hardware reliability requirements represent an expansion of the reliability requirements of the systems important to safety. They shall include a description of the types of failure which have to be tolerated without loss or with a defined and limited loss of function. In this context, the term reliability is applied to the safety of the plant and its operational availability.

5.3.2 No single random hardware failure shall prevent directly or indirectly the safety actions of the safety systems.

5.3.3 To support the system level safety analysis, an analysis of failures shall be made during design. Proper consideration for the potential for common-mode or common cause failures shall be included in this analysis.

5.3.3.1 Reliability and safety assessment shall begin as soon as the design starts. The methods which can be used for this purpose are:

a) Fault-tree analysis, which is concerned with the identification and analysis of conditions and factors which cause or contribute to the occurrence of a defined undesirable event.

b) Failure mode effects analysis, which identifies failures which have significant consequences affecting the system performance, for example, reliability, safety, availability [*see* IS 11137 (Part 2)].

5.3.3.2 It is noted that a safety analysis at the system level (hardware and software) can be done through an extension of the fault-tree analysis method. Special consideration shall be given to the effects of safety analysis document shall be generated for peer review:

a) Failure in memories;

b) Power failure and subsequent re-start and adaptation procedure;

c) Failures of sub-systems which share a bus or other resources with other sub-system and defined actions during such occurrences;

d) Electromagnetic interference;

e) Nuclear radiation; and

f) Deviation from specified ambient condition.

Any changes shown to be necessary for nuclear safety shall be implemented.

5.3.4 Strategies and provisions to assure reliability over the whole lifetime of the computer system shall be defined.

These measures shall be laid down as maintenance requirements, which form part of the reliability requirements.

They shall include requirements for:

a) Maintenance actions;

b) Replacement of sub-systems, modules and components;

c) Revalidation; and

d) Facilitating backfitting.

5.3.5 In order to meet the reliability requirements, the computer system shall supervise itself by software means. For self-supervision, *see* **5.7** and **A-2.8** of IS 15398 are applicable.

Failures which cannot be made self-annunciating by these tests shall be identified and methods specified by which the failures will be detected.

Hardware features necessary to support the design and performance of self-check may include:

a) Error detection/correction devices for memories;

b) Error detection devices for busses;

c) Instruction repetition on error detection;

d) Runtime supervision;

e) Memory management with protection of parts of the memory;

f) Redundancy on the component level in connection with voting logic; and

g) Provision for access control to system.

5.3.6 The required reliability of the system and the sub-systems shall be classified according to its importance to safety.

5.3.7 The system shall be designed to allow maintenance activities to be carried out at ease or without affecting the operation of other healthy systems. The hardware requirements should give figures for the major maintenance parameters (such as, mean time to repair, maintainability, and mean time to revalidate) and specify the requirements for methods or provisions by which the appropriate maintenance activities and targets are achieved.

These methods may include in-service accessibility, modularity, fault traceability to replaceable units, fault indicators, logging and evaluation of operation and fault history.

The hardware maintainability requirements shall be defined using as a background the reliability requirements of the nuclear power station.

5.4 Environmental Requirements

5.4.1 The hardware environmental requirements shall include location, climatic, seismic, chemical, electrical and radiation conditions where the computer system is operated. Special consideration shall be given to the environment before and during installation and start-up.

5.4.2 The electrical environment in which the computer is located may be affected by a wide variety of electrical interference sources, for example, switchgear, contactors, relays, walkie-talkies, electrostatic discharges, lightning, earth faults.

5.4.3 The degree of immunity to magnetic, electrical and electromagnetic interference shall be specified and tested according to suitable Indian Standards chosen from IS 14700 series.

5.4.4 The test severity levels for sub-systems shall be selected in accordance with the most realistic installation and environmental conditions.

5.4.5 The hardware requirements shall include any environmental conditions imposed on the choice of part types, special materials to be used or particular types of production processes and testing strategies.

5.5 Documentation Requirements

5.5.1 The hardware documentation requirements are part of the documentation requirements of the computer systems. They shall define the documentation to be produced with the product and shall include agreed procedures:

a) to identify parts of the documentation itself and ensure that the documentation is kept up to date;

b) to identify signals and components of the system;

c) for the description of functions important to safety;

d) for the description of functions in the operators' manuals and in the maintenance manuals;

e) to describe contents and boundaries of functional units (modules);

f) to modify documentation; and

g) to carry out routine and preventive maintenance check lists.

5.5.1.1 The computer system configuration shall be described using as a background, the reliability requirements of the system and the environment, since reliability properties and system configuration are closely connected.

5.5.1.2 The interface between the computer system and any other systems either within or outside the nuclear plant, wherever a direct connection exists or is planned, shall be identified and documented, indicating the specific interfaces and related hardware requirements.

5.5.1.3 The constraints which the hardware and software impose on each other shall be described.

5.5.1.4 The constraints on the hardware of any special operating conditions shall be described (*see* **5.7** and **A-2.7** of IS 15398).

5.5.1.5 System acceptance documents for transferring to user shall be prepared.

6 DESIGN AND DEVELOPMENT

6.1 General

6.1.1 This clause is applicable to system, sub-system and module levels as appropriate. Design and development are interactive with one another and shall conform to the hardware requirements specification.

6.1.2 Design and development starts from the hardware requirements specification, goes through stages of different levels of detail and ends with a definition of a product which has been shown to meet the hardware requirements specification. During each stage, the activities follow the same framework (*see* Annex B).

6.1.3 The more general level of design activity is the preliminary design, which consists of the analysis of different design alternatives in order to define the hardware system architecture in terms of sub-systems and modules.

6.1.4 Preliminary design is followed by one or more detailed design levels. The detailed design activity expands the preliminary design to contain more detailed descriptions on the sub-system, module and component levels to the extent that the design description is sufficiently complete to be implemented.

6.1.5 It is usual to build a set of prototype hardware, not only to demonstrate successful interaction between modules, but also to enable both hardware and software to be operated together in order to demonstrate their compatibility.

6.1.6 In some cases, off-the-shelf available equipment (for example, hardware with built-in programmes and implementation tools) may exist for the development and design of the system or parts of it. In this case, evidence shall be provided that this equipment is qualified (*see* Annex B of IS 15398) and that its scope conforms to the design requirements.

NOTE — In this context, built-in programmes are the computer programmes that are an inherent part of the computer equipment for the operation of the computer or for generic application functions, while application programmes are computer programmes that are unique to the specific application. Built-in programmes, together with application programmes, form the whole set of computer programmes.

6.2 Design Activities

6.2.1 All the characteristics of the performance of the system which are defined in the hardware requirements shall be analysed and stated in the design documentation and evidence shall be made available to show that the design has at least the performance characteristics listed. Such characteristics include accuracy, time response, cycle time environmental conditions, electrical supply requirements and characteristics of input signal, such as, range, noise, type, etc.

6.2.2 Anything affecting the compliance with the hardware requirements shall be brought to the attention of those responsible for the hardware requirements.

6.2.3 The designers shall carry out and record such tests as are necessary to show that the required performance has been achieved. For further testing of the integrated system, **8.5** of IS 15398 is applicable.

6.2.4 The designers shall specify the maintenance activities needed to meet the performance and reliability requirements. This may cover operational tests, calibration, repair, replacement periodicity and procedures.

6.2.5 Evidence shall be made available to show that the specified qualified life will be achieved.

6.3 Reliability Criteria

Estimates shall be made of the reliability of sub-systems, modules and components which may affect nuclear safety and shall be compared with the corresponding hardware reliability requirements to identify and correct deficiencies.

6.3.1 Redundancy and diversity should be used to meet the required reliability. Fault tolerant units at the lowest level possible should be preferred.

6.3.2 When redundancy or diversity is used, the design shall provide adequate independence of systems and sub-system and shall aim to achieve least common mode failures. For example, power supplies should be from different sources and physical separation should guard against the effects of fire. A policy of obtaining components from more than one supplier may be applied.

6.3.3 The design shall provide facilities which make

maintenance easy as far as is compatible with reliability goals. For example, fault annunciation, fault diagnostic features, simple module replacement and in-the-field testing capabilities should be provided.

6.4 Interfaces

6.4.1 No systems of lower safety relevance shall be allowed to influence the performance of a system of higher safety relevance. It shall be demonstrated in particular that no hardware and no software failure of the system of lower safety relevance can, for example, destroy data or increase cycle times of the system of higher safety relevance.

6.4.2 The design should be made to be compatible with other systems used on the same plant. The system shall also be protected against damage or malfunction as a result of failure in the systems or features of the systems with which it shares an interface. This applies also to the user interface.

6.5 Modification

The design shall be capable of being modified to meet changed functional requirements within the spare capacity specified, according to national regulations or company practice, or to overcome design faults (*see* **12**).

6.6 Power Failure

The computer system shall be made as insensitive as possible to the consequences of short-term power failures of the guaranteed power supply. Means shall be provided for operators and maintenance staff to be made aware of such power failures. Non-volatile, non-erasable or read-only memories are preferred as is automatic programme reloading where appropriate. Design should ensure that safety critical thresholds, processing routines, passwords, major keywords, etc., are not affected during power failures.

6.7 Component Selection

The characteristics of the components used in the design which are important to its function shall be specified. The components shall be available to an appropriate quality standard. Components should be chosen from a list of preferred components. The quality of new components or new assembly techniques to be used shall be investigated and proven by following applicable/relevant qualified test methods.

6.8 Design Documentation

The hardware design documentation describes the hardware system and the method by which the implementation will meet the hardware requirements specification. The hardware description, including preliminary and final description shall be produced by the designers. Standardized forms of documentation and automated design tools should be preferred.

The detailed design documentation of each level includes the detailed design of the components defined at that level and the hardware requirements for components of lower level. Documents for manufacturing, installation, commissioning, maintenance and operation shall be available at the end of detailed design. They need not include all manufacturing instructions but they shall include all manufacturing, maintenance and operating information which is important to meeting the hardware requirements specification.

6.8.1 *Preliminary Description*

The preliminary description defines the hardware architecture, that is the structure and relationship between the parts of the system. It includes the general layout of hardware with block diagrams of sub-systems and modules of lower level. It includes also hardware requirements for the detailed design, such as:

a) Number and types of central processor units and other processors;

b) Number, types and capacities of memories;

c) Number and types of interfaces; and

d) Number and types of data links and busses.

6.8.2 *Final Description*

At the conclusion of the design and development of the hardware system, a final description shall be available that conveys both the design details down to the lower level and the requirements, design principles, capabilities, limitations and other characteristics of the hardware.

The corresponding documents shall include:

a) An overview defining the boundaries of the hardware to be described in detail.

b) Cross-reference to the system design and software descriptions.

c) The sub-division of the system in terms of physical sub-systems. Each sub-system is described in terms of its major modules and components.

d) The sub-system and module structure (block diagrams, circuit diagrams at gate level).

e) The sub-system interfaces. Interfaces are described as appropriate in logical, physical electrical or other terms.

f) The computer system interfaces, interfaces with any other systems either within or outside the nuclear plant, wherever a direct connection exists or is planned, shall be identified showing the specific interfaces and related hardware requirements.

g) The physical layout. A description with diagrams of the physical layout of the equipment should be provided.

h) Qualification data (*see* **8**).

j) The approach to reliability and safety. This should describe how the requirements for system reliability and fail-safe properties are fulfilled by the hardware.

7 VERIFICATION AND VALIDATION

The design and development process shall include formal checks that the hardware at each phase of design and development meets the requirements imposed by the previous phase. In order to ensure maximum efficiency, verification shall be applied from the beginning of the hardware development programme and not during the testing phase alone.

The amount of verification performed will depend upon the importance of the system to plant safety and the effects of system failure. For example, hardware used in safety systems should have a more stringent verification programme than that used in safety-related systems.

The hardware verification phase starts with verification of the hardware design requirements against the system performance requirements and ends when the application software is integrated with the hardware. For verification requirements for the hardware/software integration phase of system development, *see* **8.5** of IS 15398.

The design of hardware modules may also be subjected to formal verification process by soft simulation technique using tools like multisun, P-spice and HDL modules etc.

7.1 Verification Plan

A formal verification plan shall be prepared by the verification personnel to document the approach used to verify the hardware design and to control the verification process. The plan shall be prepared prior to initiating verification actions. The plan should document the verification organization structure, verification methods to be used, level of verification to be performed, schedules and other significant project activities related to verification.

a) Verification should be performed in parallel with the design process in order that errors may be detected and corrected as soon as possible.

b) Formal verification actions shall not take place until the design or part of it is released for verification by the design personnel. Once released for verification, the design and related documentation shall be maintained under formal change control. This should be compatible with **8** and **9** of IS 15398.

c) After release for verification, all changes to the design shall be submitted to the verification personnel for review. The verification personnel shall determine the need for additional verification.

7.2 Independence of Verification

Individuals or groups who perform the design verification shall be independent from those who are involved in the design activity. Persons involved with verification may be from the same organization as the individuals responsible for the design:

a) The skills of verification personnel shall be similar to the skills of the people who carried out the design.

b) Communications between the design and verification personnel shall be formally documented to allow traceability of the verification activities.

c) The persons responsible for verification shall determine and document the level of verification to be performed.

7.3 Methods

Critical reviews, audits, analysis, tests or a combination of these methods may be used to provide design verification. The basis for the choice of verification method to be used shall be documented with enough detail to allow auditing by personnel who are not directly involved in the design or verification activities.

a) The choice of verification method should consider the following:

1) The safety-related classification of the system (safety system or safety-related system);

2) Reviews and tests performed as part of the normal design and quality control processes with documentation available to support verification;

3) Previous verification activities performed on similar hardware or systems;

4) System size, maturity and complexity; and

5) Data which may be available from other sources such as quality assurance or environmental qualification processes.

b) Verification personnel shall choose the test tools and instruments to be used in the verification programme. Appropriate tools and methods shall be provided for the testing of sub-systems and electronic components to ensure that they can be thoroughly tested. Automatic test tools should be used to provide for reproducibility and documentation of test results, and to reduce the probability of human errors during the test.

c) Test instruments or test tools used in the verification or testing process shall be calibrated and appropriately validated. A record

shall be made to show that valid calibrations are in effect at the same time as the device is used.

7.4 Documentation

All verification activities shall be formally documented with sufficient detail to allow auditing by persons not directly involved in the development and verification programme. This includes documentation of the verification programme plan, requirements, test procedures, test results, results of a review of design changes and any discrepancies which are discovered during the hardware verification process.

a) Test procedures should be clearly written, provide step-by-step instructions for hardware verification and should contain detailed information of the test set-up.

b) Test procedures shall contain unambiguous pass/ fail criteria.

c) Test procedures implemented by software shall be documented and integrated in the test documentation.

7.5 Discrepancies

Discrepancies found during the verification process shall be formally documented and transmitted to the design personnel for resolution. The response of the design personnel shall be formally documented to provide a traceable path to assure that all discrepancies are responded to and all deficiencies are corrected.

7.6 Changes and Modifications

Once successfully completed, verification is not required to be repeated as long as the computer system requirements are not changed. For changes to the verified design **7.1** (c) is applicable.

Modified parts should be identified in accordance with the specified quality control procedures.

7.7 Installation Verification

Verification of correct system installation shall be in accordance with **10**.

7.8 Validation

Testing shall be performed to validate the software and hardware as a system which complies with the requirements of the systems important to safety to be satisfied by the computer system. For this validation, **9** of IS 15398 is applicable.

8 QUALIFICATION

The computer system hardware shall be qualified according to a suitable national or international standard. Qualification may be achieved at a number of phases during development. An outline of qualification is given in Annex C.

9 MANUFACTURE

The sub-systems, modules and components to be used in the computer system include off-the-shelf products and dedicated hardware products built in accordance with the final documents. **4.2** of IS 15398 is applicable to quality assurance for both classes.

10 INSTALLATION AND COMMISSIONING

10.1 Packing, handling, transport, storage and unpacking shall be such as to prevent any damage to the system.

10.2 Before the system is unpacked and installed, the environment in which the system is to be installed shall be verified to conform to the hardware environmental requirements of **5.4**.

10.3 Adequate procedures and information shall be available to enable the system to be installed, cabled and wired in accordance with the design requirements, in particular with regard to the earthing requirements, identification of items of equipment shall form part of this information. For this purpose, a quality plan shall be applied. The system shall be installed, cabled, tested and set to work in accordance with defined procedures.

10.4 The proper working of the system at site shall be checked by planned and specified commissioning tests. A commissioning test plan, consisting of acceptance criteria, test cases and test environments, shall be established.

For each sub-system, tests shall be carried out to demonstrate its correct function.

a) Any defect due to design errors or any change to improve the system performance shall be recorded. A formal procedure according to **11**, shall be used to control the necessary changes.

b) Any defect due to manufacturing errors shall be recorded. Defective parts shall be replaced only by new parts which have undergone factory testing. The manufacturing process and the factory testing shall be investigated and changed, if necessary to avoid further delivery of defective parts.

c) Any defect due to errors in installation, cabling or wiring shall be corrected and recorded.

10.5 The immunity of the computer system to electromagnetic interference shall be tested in the final installed conditions.

The tests shall be performed in accordance with suitable Indian Standards chosen from IS 14700 series.

The severity level of electromagnetic interference shall be chosen such that it conforms to the worst conditions to which the system may be subjected.

10.6 On the completion of installation and commissioning, it is necessary to carry out the process of acceptance before the system is transferred to the user.

11 MAINTENANCE

Hardware maintenance comprises:

a) Tests, checks and calibration which may be either periodic within specified maximum intervals or after replacement, exchange, overhaul and repair (revalidation);

b) Maintenance, such as, is required to maintain the computer hardware in good working order, replacement of expendables and the preventative exchange and overhaul of equipment, sub-units, parts and components; and

c) Repairs, the restoration of the operability of failed equipment, sub-units and parts.

11.1 Maintenance Requirements

a) A formal procedure shall be specified and applied to control the execution and the documentation of maintenance (*see* Annex D).

This shall take into account:

1) Organizational preparations if the maintenance activities affect plant operation; and

2) Operational preparations of the systems important to safety and of plant components.

b) Maintenance shall be undertaken by qualified and authorized personnel only. It shall be recorded according to a specified procedure. The procedure shall make provision for personal certification by an authorized person that each task has been completed satisfactorily.

Other relevant information, such as, time and date, replacements fitted, etc, shall also be recorded. National or customer authorization documentation practice should be followed.

c) Maintenance work shall be subject to audits.

d) Satisfactory operation in service depends upon the application of controls to ensure that parts are replaced after a period of time not longer than the qualified life and that the replacement parts are of a quality appropriate to their duty. The suppliers of components, modules, sub-systems and the systems in total shall be shown to intend to continue to provide such replacement.

Spare parts shall be kept in a store whose atmosphere is controlled with regard to temperature, humidity, gases and particles. The store shall be constructed in such a way that the effects of fire on the spare parts are minimized. The shelf life of spare parts shall be controlled within specified intervals according to maintenance instructions.

e) Only spares qualified according to 7 shall be used.

f) Replacement parts in general as well as modified replacement parts shall be identifiable above component level.

11.2 Failure Data

Consideration shall be given to the derivation of failure data statistics from the equipment repair records.

Failure data acquisition during equipment operation constitutes a major source of information which can be used to improve:

a) Component reliability data knowledge by taking into account real operating environment conditions;

b) Equipment reliability evaluations by determining actual field failure data and by observing availability in operating conditions; and

c) Maintenance policy through better spare parts optimization, preventative maintenance schedules and maintenance personnel requirements.

Accordingly, field failure data should be logged in a failure data bank using information available from maintenance reports.

The maintenance reports shall contain:

a) Equipment identification;

b) Description of fault;

c) Reference to eventual problem report;

d) Date of intervention;

e) Intervention duration;

f) Failure component identification with eventual primary failed component (origin of a cascade of component failures);

g) Component age;

h) Component localization; and

j) Failure circumstances and failure effects.

NOTE — Suitable standards chosen from IS 7354 series and IS 9692 series may be used to provide a methodology for reliability measurements.

11.3 Maintenance Documentation

Instructions for maintenance shall be provided in written form by means of procedures, manuals, handbooks, etc.

Maintenance documents shall describe maintenance policy for the type of hardware components which are checked and when they are re-checked or substituted [*see* **11.1**(e)].

Maintenance documents shall describe the way in which failure of each specific module of the system is made apparent and diagnosed.

Maintenance documents shall describe repair policy, that is:

a) the methods of repair or substitution of different sub-systems, modules and components;

b) the restrictions to which the system is subjected during repair time (for example, the system or parts of the system which shall be switched off); and

c) the extent to which the system shall be revalidated after a repair.

In addition to the procedures for scheduled periodic maintenance, procedures shall be provided to be used for cases where anomalous system behaviour leads to suspicion of failure or design error.

12 MODIFICATION

Hardware modification may be required to correct defective performance or to cater to new or revised performance requirements.

Any change necessary to fulfil additional or changed requirements shall be brought to the attention of those responsible for the hardware requirements.

12.1 Hardware changes made during design shall be controlled by a formal procedure. The procedure should be compatible with the procedure used to control software changes and should ensure that the modified parts are identified in accordance with the specified quality control procedure.

12.2 A formal procedure shall be used to control design and hardware changes to the original approved design or test intent. The procedure should be compatible with **8** and **10** of IS 15398 as well as with the procedure used to control software design changes.

12.3 The effect of the modification on the software shall be examined according to **10.3.3** of IS 15398.

12.4 The changed hardware shall be shown to meet the hardware/software integration requirements specification clause.

12.5 The changed hardware shall be shown to meet the hardware requirements as per **5**.

12.6 For the verification of changed hardware, **7.1**(c) and **7.4** are applicable. In cases where the verification personnel for the original design are not available, the requirements of **7.2** with regard to the verification personnel shall be met accordingly.

12.7 Modifications after commissioning and acceptance shall follow a formal procedure. Depending on the kid of modification, it may be necessary to return to the detail design phase or even to the system level.

13 OPERATION

13.1 In addition to the requirements of **11** of IS 15398, the following requirements are applicable to the operation of the computer system. A method of controlling the authorization of manuals, procedures and personnel shall be applied in accordance with national regulations and practice.

13.2 Operating procedures shall include activities to be followed in circumstances not explicitly provided for in order to bring these situations to the attention of an authorized person or group of persons to determine what is to be done.

13.3 Any decision to deviate from an authorized procedure shall be made only by an authorized person or group of persons, and shall be comprehensively documented.

13.4 The requirements of **11.3** shall apply to the operating procedures.

13.5 All persons classed as authorized persons shall be properly trained before authorization and a formal certification system applied. A system of periodic re-training and re-certification may be provided if it is possible for the original certification to be in doubt, for example, following a temporary assignment to a different kind of work or major changes to the installed equipment. The term authorized persons is used in this connection to describe all who are specifically authorized to carry out particular duties in relation to the plant. It includes operating staff, maintenance and repair personnel.

14 DOCUMENTATION

The hardware documentation is part of the documentation of the computer system and shall be controlled by quality assurance procedures.

The hardware documentation shall cover all aspects from requirements (*see* **5.5**) through design (*see* **6.8**), verification (*see* **7.4**), maintenance (*see* **11.3**) and operation (*see* **13**).

All significant procedures and instructions shall be defined in formal documents. Procedures and instructions are classed as significant if their incorrect execution can cause the system to fail to meet its hardware requirements specification.

A list of all applicable procedures and instruction documents together with the latest state of amendment of each shall be available to all operators and maintenance staff.

14.1 Documentation Presentation

The significant documentation shall be structured, cross-referenced and indexed. Documents shall be worded unambiguously and use the smallest vocabulary consistent with clear understanding.

14.2 Documentation Control

The hardware requirements documentation shall be updated and re-issued when necessary throughout the project in order to encompass new or changed information which may appear at any stage in the project or as a result of feedback compatibility checks between hardware and software:

a) Specified procedures for amending documentation shall be used and be part of the project operation and maintenance procedures.

b) The documentation shall be handled according to specified procedures (including responsibilities, file copy, distribution to and updating work copy, etc).

c) All significant documents should carry a formal certification of their state of amendment and the status of their authorization. This information shall be given either on the front cover or on the first page.

d) Controls shall be exercised over changes to the system documents to ensure that:

1) Necessary amendments are made to the copies used by design, installation, commissioning, operating and maintenance staff, and

2) Amendments which do not apply to the particular set of equipment are not inserted.

Automatic tools may be used in this context.

ANNEX A

(*Clause* 2)

LIST OF REFERRED INDIAN STANDARDS

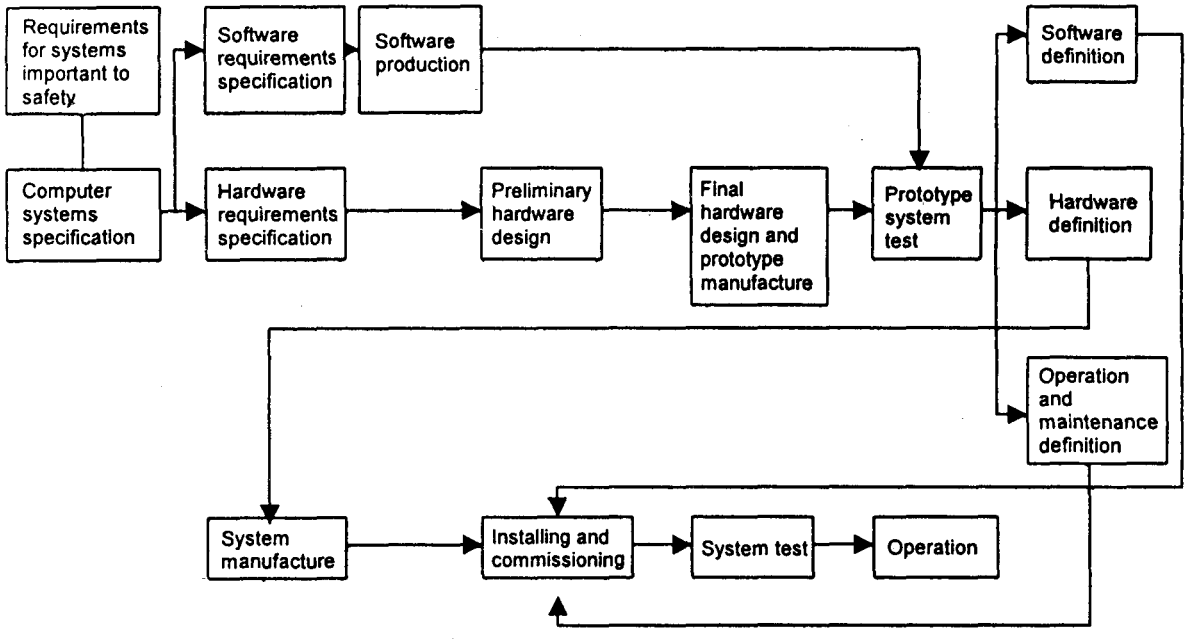
IS No.	*Title*
IS 7354	Guide on reliability of electronic and electrical items:
(Part 1) : 1975	Preliminary reliability considerations
(Part 2) : 1984	Reliability and maintainability management (*first revision*)
(Part 3) : 1984	Presentation of reliability data on electronic and electrical components (or parts) (*first revision*)
(Part 4) : 1974	Collection of reliability, availability and maintainability data from field performance
(Part 5) : 1975	Inclusion of lot-by-lot and periodic inspection procedures in specifications for electronic and electrical components (or parts) (*first revision*)
(Part 6) : 1983	Inclusion of reliability clauses into specifications for components (or parts) (*first revision*)
IS 9692	Guide on maintainability of equipment:
(Part 1) : 1980	Introduction to maintainability
(Part 2) : 1980	Maintainability requirements in specifications and contracts
(Part 3) : 1981	Maintainability programme
(Part 4) : 1987	Test and diagnostic procedures
(Part 5) : 1985	Maintainability studies during the design phase
(Part 6) : 1983	Maintainability verification
(Part 7) : 1984	Collection, analysis and presentation of data related to maintainability
(Part 8/Sec 1): 1988	Maintenance and maintenance support planning, Section 1 General
(Part 8/Sec 2): 1988	Maintenance and maintenance support planning, Section 2 Maintenance support analysis
(Part 8/Sec 3): 1988	Maintenance and maintenance support planning, Section 3 Maintenance planning analysis
(Part 8/Sec 4): 1988	Maintenance and maintenance support planning, Section 4 Maintenance support resources requirements
IS 11137 (Part 2) : 1984	Analysis techniques for system reliability : Part 2 Procedure for failure mode and effects analysis (FMEA) and failure mode, effects and criticality analysis (FMECA)

IS No.	*Title*
IS 14700	Electromagnetic compatibility (EMC):
(Part 1/Sec 1) : 2000	General, Section 1 Application and interpretation of fundamental definitions and terms
(Part 3/Sec 2) : 1999	Limits, Section 2 Limits for harmonic current emissions (equipment input current ≤ 16A per phase)
(Part 3/Sec 3) : 1999	Limits, Section 3 Limitations of voltage fluctuations and flicker in low voltage supply systems for equipment with rated current ≤ 16A
(Part 4/Sec 1) : 1999	Testing and measurement techniques, Section 1 Overview of immunity tests — Basic EMC publication
(Part 4/Sec 2) : 1999	Testing and measurement techniques, Section 2 Electrostatic discharge immunity test — Basic EMC publication
(Part 4/Sec 4) : 1999	Testing and measurement techniques, Section 4 Electrical fast transient /burst immunity test
(Part 4/Sec 8) : 1999	Testing and measurement techniques, Section 8 Power frequency magnetic field immunity test
(Part 4/Sec 9) : 1999	Testing and measurement techniques, Section 9 Pulse magnetic field immunity test
(Part 4/Sec 12) : 1999	Testing and measurement techniques, Section 12 Oscillatory waves immunity test
(Part 4/Sec 15) : 2001	Testing and measurement techniques, Section 15 Flickermeter functional and design specification
(Part 4/Sec 16) : 2001	Testing and measurement techniques, Section 16 Test for immunity to be conducted common mode disturbances in the frequency range 0 Hz to 150 kHz
(Part 6/Sec 3) : 2002	Generic standards, Section 3 Emission standards for residential, commercial and light industrial environment
IS 15398 : 2003	Software for computers in the safety systems of nuclear and radiation facilities

ANNEX B

(*Clauses* 4.2 *and* 6.1.2)

OVERVIEW OF SYSTEM LIFE CYCLE

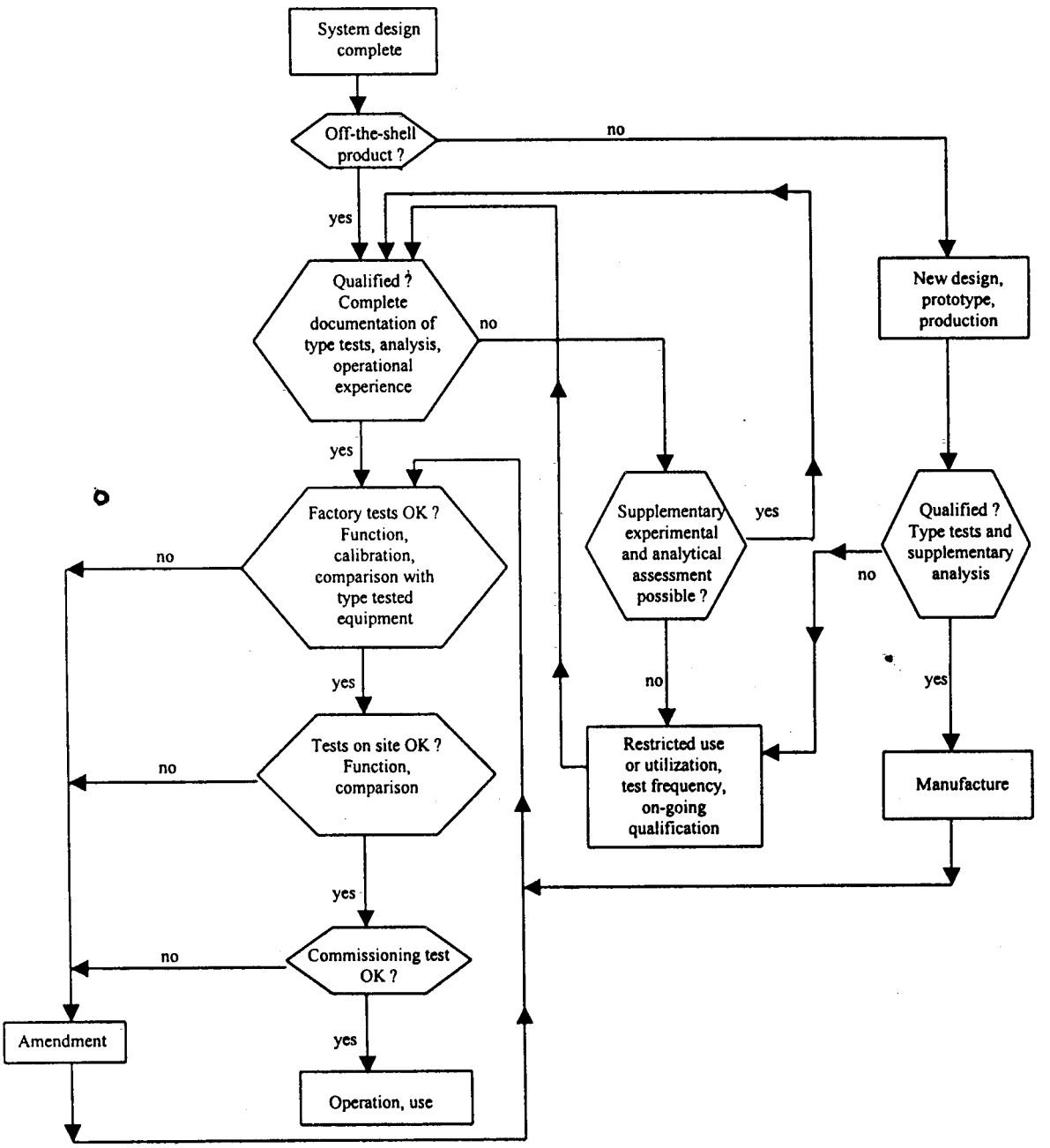


NOTE — In the interest of clarity, the feedback paths have not been shown.

ANNEX C

(*Clause* 8)

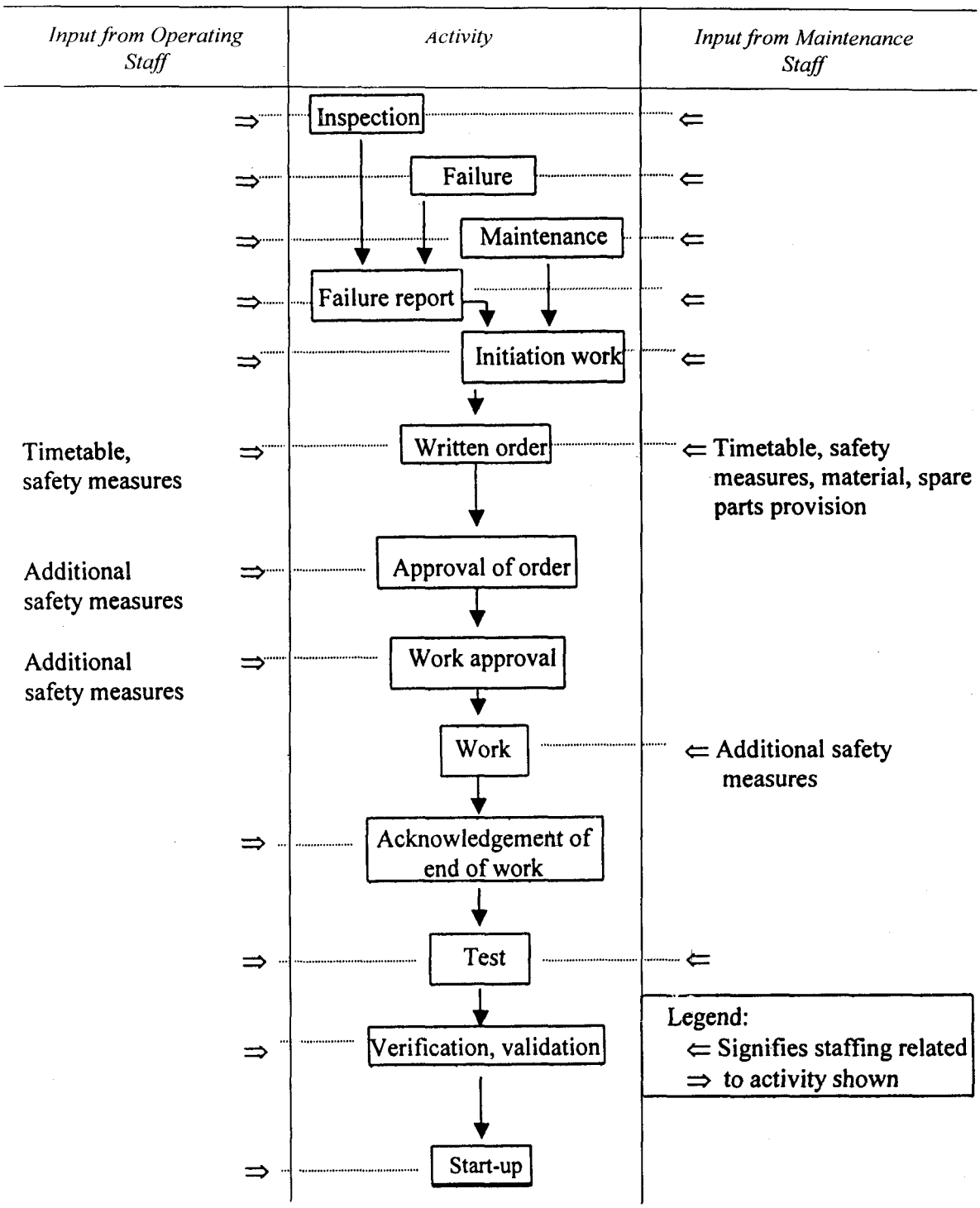
OUTLINE OF QUALIFICATION



ANNEX D

(*Clause* 11.1)

EXAMPLE OF MAINTENANCE PROCEDURE



ANNEX E

(Foreword)

COMMITTEE COMPOSITION

Nuclear Instrumentation Sectional Committee, LTD 26

Organization	*Representative(s)*
Indira Gandhi Centre for Atomic Research, Kalpakkam	SHRI P. SWAMINATHAN (***Chairman***) SHRI S. A. V. SATHYAMURTHY (*Alternate*)
Atomic Energy Regulatory Board, Mumbai	SHRI P. R. KRISHNAMURTHY SHRI P. HAJRA (*Alternate*)
Atomic Minerals Division, Hyderabad	SHRI R. SREEHARI
Bhabha Atomic Research Centre, Mumbai	DR S. K. KATARIA SHRI DEBASHIS DAS (*Alternate* I) SHRI P. K. MUKHOPADHYAY (*Alternate* II)
Centre for Advanced Technology, Indore	SHRI B. J. VAIDYA SHRI A. G. BHUJALE (*Alternate*)
Electronics Corporation of India Limited, Hyderabad	DR M. S. R. MURTY
Indian Institute of Technology, Kanpur	PROF S. QURESHI PROF P. MUNSHI (*Alternate*)
Indian Plasma Research Institute, Gandhinagar	DR ANURAG SHYAM
Ministry of Defence (DRDO), New Delhi	SHRI G. C. BHOLA
Nuclear Power Corporation, Mumbai	SHRI S. RAMAKRISHNAN SHRI R. Y. APTE (*Alternate*)
Nuclear Science Centre, New Delhi	DR R. K. BHOWMIK
PLA Electro Appliances Ltd, Mumbai	SHRI N. R. SHAH SHRI K. K. M. NAIR (*Alternate*)
Saha Institute of Nuclear Physics, Kolkata	DR SUVENDU BOSE DR PRATAP BHATTACHARYA (*Alternate*)
Variable Energy Cyclotron Centre, Kolkata	SHRI N. K. MUKHOPADHYAY
BIS Directorate General	SHRI VIJAI, Director & Head (LTD) [Representing Director General (*Ex-officio*)]

Member Secretary
SHRI PRAVEEN KUMAR
Deputy Director (LTD), BIS

Bureau of Indian Standards

BIS is a statutory institution established under the *Bureau of Indian Standards Act*, 1986 to promote harmonious development of the activities of standardization, marking and quality certification of goods and attending to connected matters in the country.

Copyright

BIS has the copyright of all its publications. No part of these publications may be reproduced in any form without the prior permission in writing of BIS. This does not preclude the free use, in the course of implementing the standard, of necessary details, such as symbols and sizes, type or grade designations. Enquiries relating to copyright be addressed to the Director (Publication), BIS.

Review of Indian Standards

Amendments are issued to standards as the need arises on the basis of comments. Standards are also reviewed periodically; a standard along with amendments is reaffirmed when such review indicates that no changes are needed; if the review indicates that changes are needed, it is taken up for revision. Users of Indian Standards should ascertain that they are in possession of the latest amendments or edition by referring to the latest issue of 'BIS Catalogue' and 'Standards: Monthly Additions'.

This Indian Standard has been developed from Doc: No. LTD 26 (1999).

Amendments Issued Since Publication

Amend No.	Date of Issue	Text Affected

BUREAU OF INDIAN STANDARDS

Headquarters:

Manak Bhavan, 9 Bahadur Shah Zafar Marg, New Delhi 110002
Telephones: 2323 0131, 2323 3375, 2323 9402

Telegrams: Manaksanstha
(Common to all offices)

Regional Offices:		Telephone
Central	: Manak Bhavan, 9 Bahadur Shah Zafar Marg, NEW DELHI 110002	2323 7617, 2323 3841
Eastern	: 1/14 C.I.T. Scheme VII M, V.I.P. Road, Kankurgachi, KOLKATA 700054	2337 8499, 2337 8561, 2337 8626, 2337 9120
Northern	: SCO 335-336, Sector 34-A, CHANDIGARH 160022	60 3843, 60 9285
Southern	: C.I.T. Campus, IV Cross Road, CHENNAI 600113	2254 1216, 2254 1442, 2254 2519, 2254 2315
Western	: Manakalaya, E9 MIDC, Marol, Andheri (East), MUMBAI 400093	2832 9295, 2832 7858, 2832 7891, 2832 7892

Branches : AHMEDABAD. BANGALORE. BHOPAL. BHUBANESHWAR. COIMBATORE. FARIDABAD. GHAZIABAD. GUWAHATI. HYDERABAD. JAIPUR. KANPUR. LUCKNOW. NAGPUR. NALAGARH. PATNA. PUNE. RAJKOT. THIRUVANANTHAPURAM. VISAKHAPATNAM.

Printed at Simco Printing Press, Delhi